

# ABSTRACT OF THE DISCLOSURE

A random number generating unit generates a random number  $t$ .  
An elliptic curve setting unit defines an elliptic curve  $E: y^2 = x^3 - 3x + t$ . An elliptic curve finitude judging unit judges  
5 whether orders  $m1$  and  $m2$  of respective elliptic curves  $Ep1$  and  $Ep2$  produced by reducing the elliptic curve  $E$  on a rational  
number field modulo primes  $p1$  and  $p2$  are relatively prime. An  
elliptic curve order computing unit computes an order of the  
elliptic curve  $E$ . An elliptic curve condition judging unit  
10 judges the security of the elliptic curve  $E$  based on the computed  
order.